Como criar chaves no Windows

Como pré-requisito, é preciso ter dois programas instalados em seu computador:

PuTTYgen - esse é o programa que irá gerar as chaves públicas e privadas.

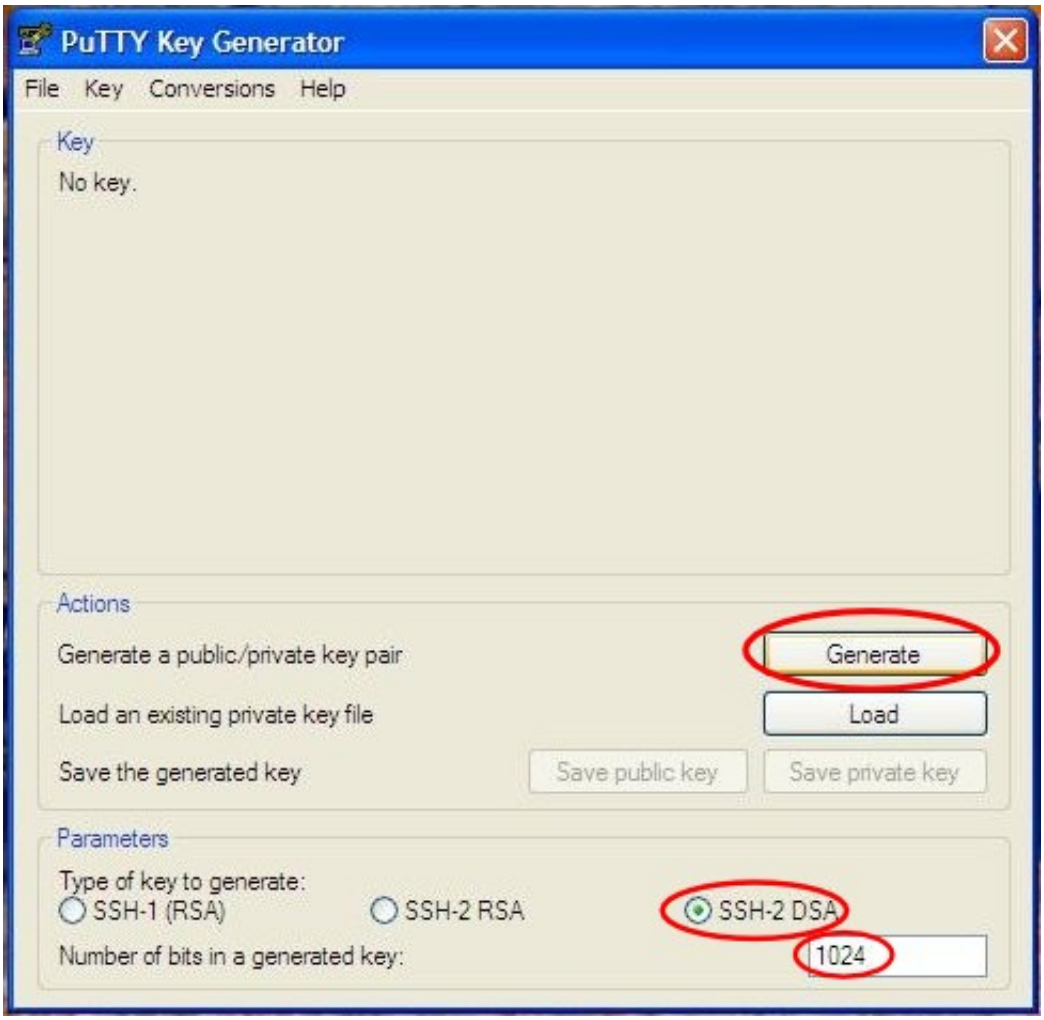
Pageant - esse programa faz a autenticação do par de chaves para o PuTTY e para o PSCP.

Você pode consegui-los no endereço abaixo individualmente ou juntos (através do instalador para Windows) que instala a maioria dos utilitários listados no site:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

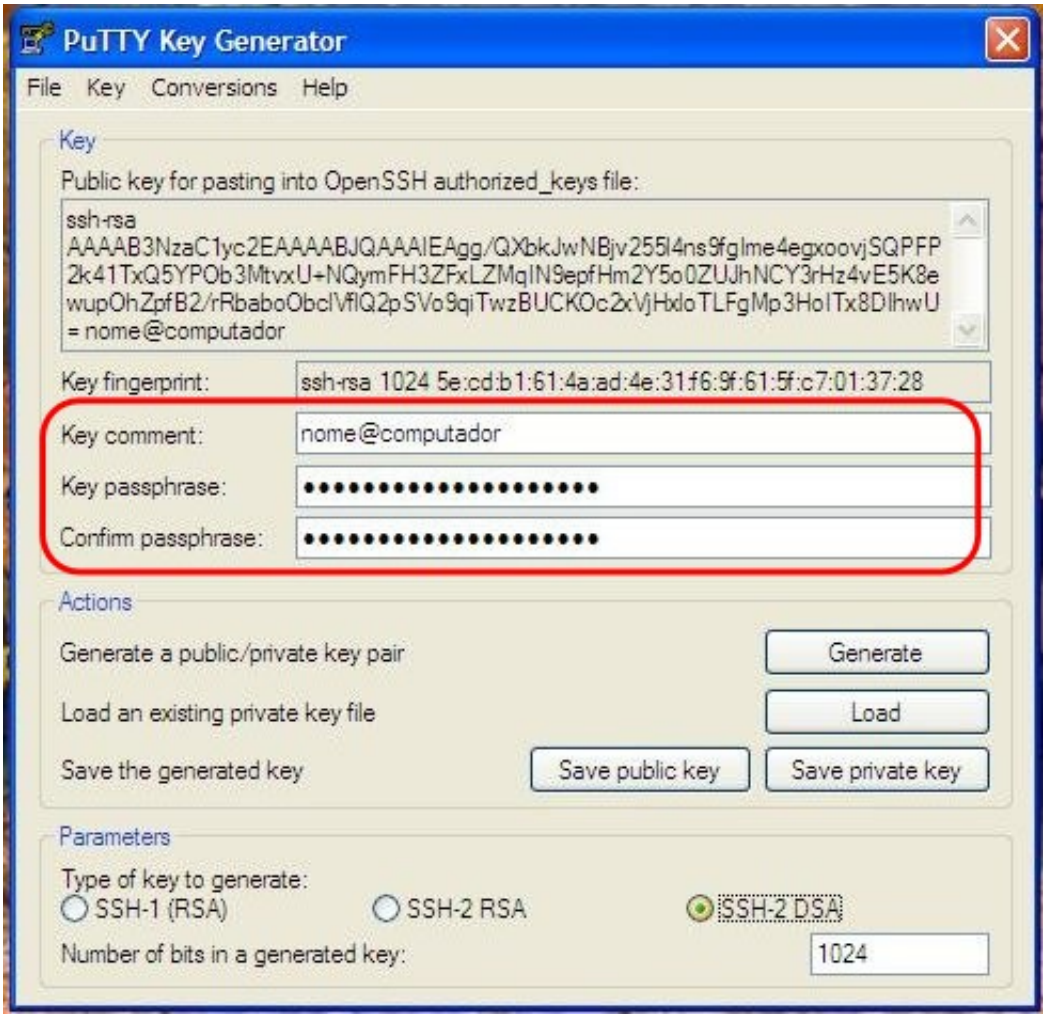
Uma vez instalados, inicie o programa PuTTYgen. A tela que aparecerá será como a mostrada abaixo:

Certifique-se de que o campo Number of bits in a generated key contenha o valor 1024. Escolha a opção SSH-2 DSA e clique no botão Generate. O programa esperará que você mexa com o mouse aleatoriamente sobre a janela do programa para que o par de chaves seja gerado. A medida que você mexe com o mouse, uma barra de progresso vai se completando.



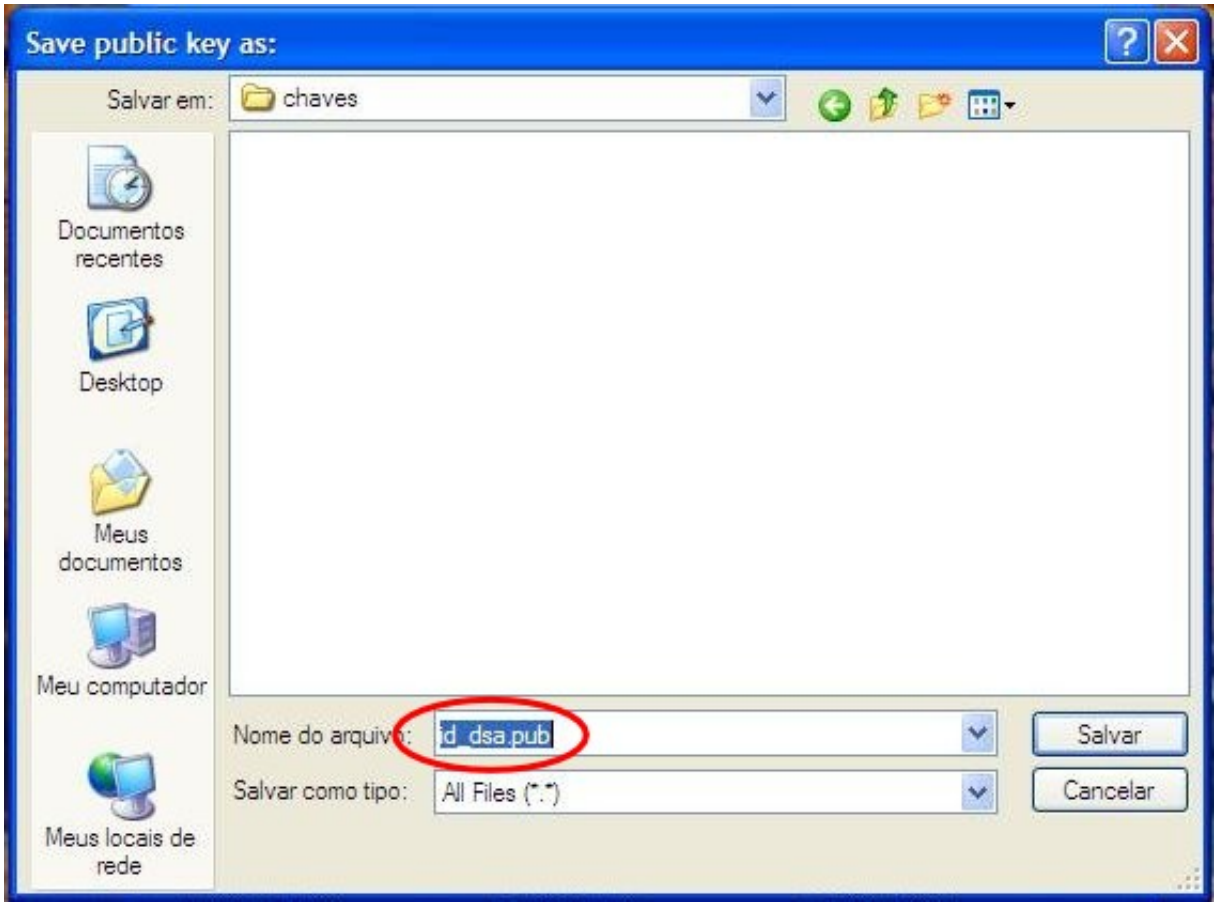
Geradas as chaves, é aconselhável mudar os campos Key comment e Key passphrase. O primeiro campo citado é um comentário que identifica a chave. No Linux, a parte das chaves que corresponde a esse campo vem com o nome do usuário seguido de uma @ (arroba) e o nome da máquina que gerou as chaves. Para melhor organização, sigamos o mesmo modelo das máquinas Linux.

O segundo campo citado, Key passphrase, é a chave-senha para seu acesso. Com esse campo preenchido dificulta-se as invasões em quaisquer máquinas por pessoas mal intencionadas. Você pode/deve colocar algo como “batatinha quando nasce esparrama pelo chao“.

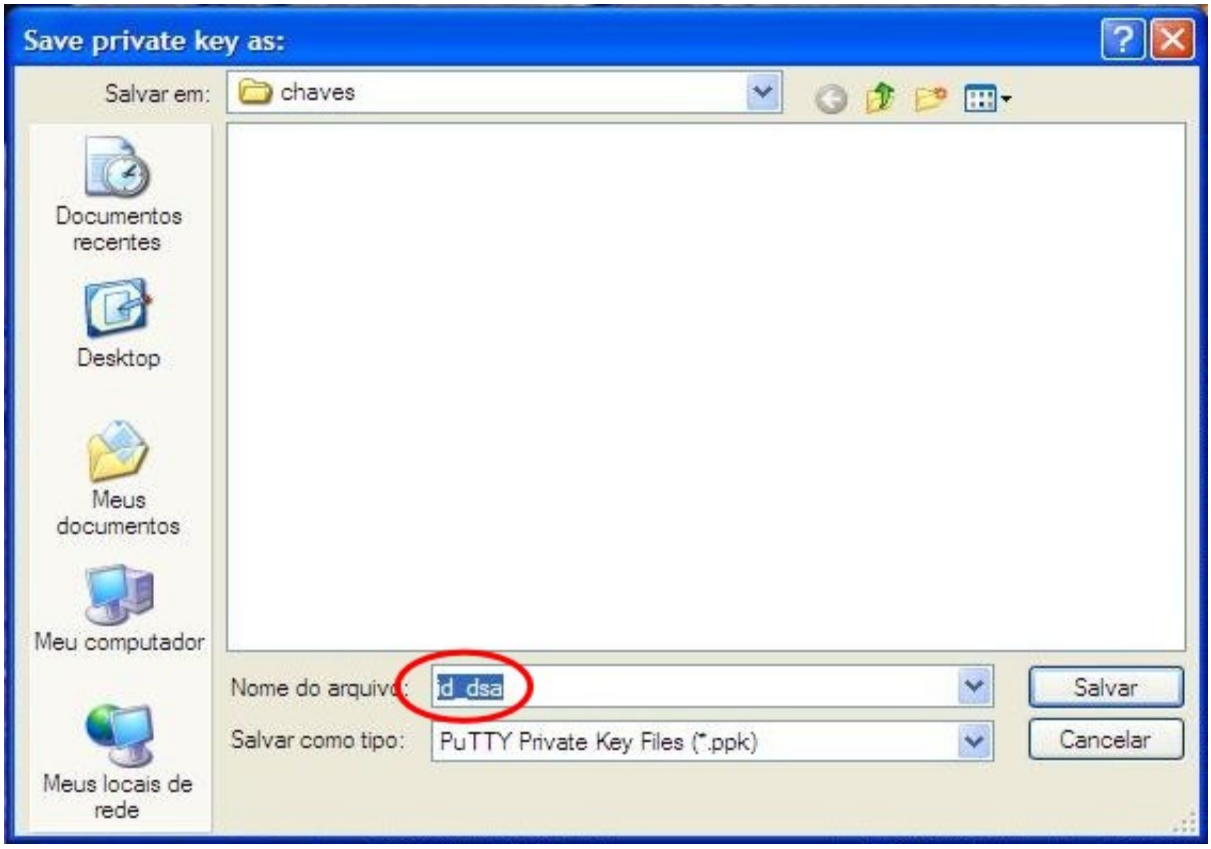


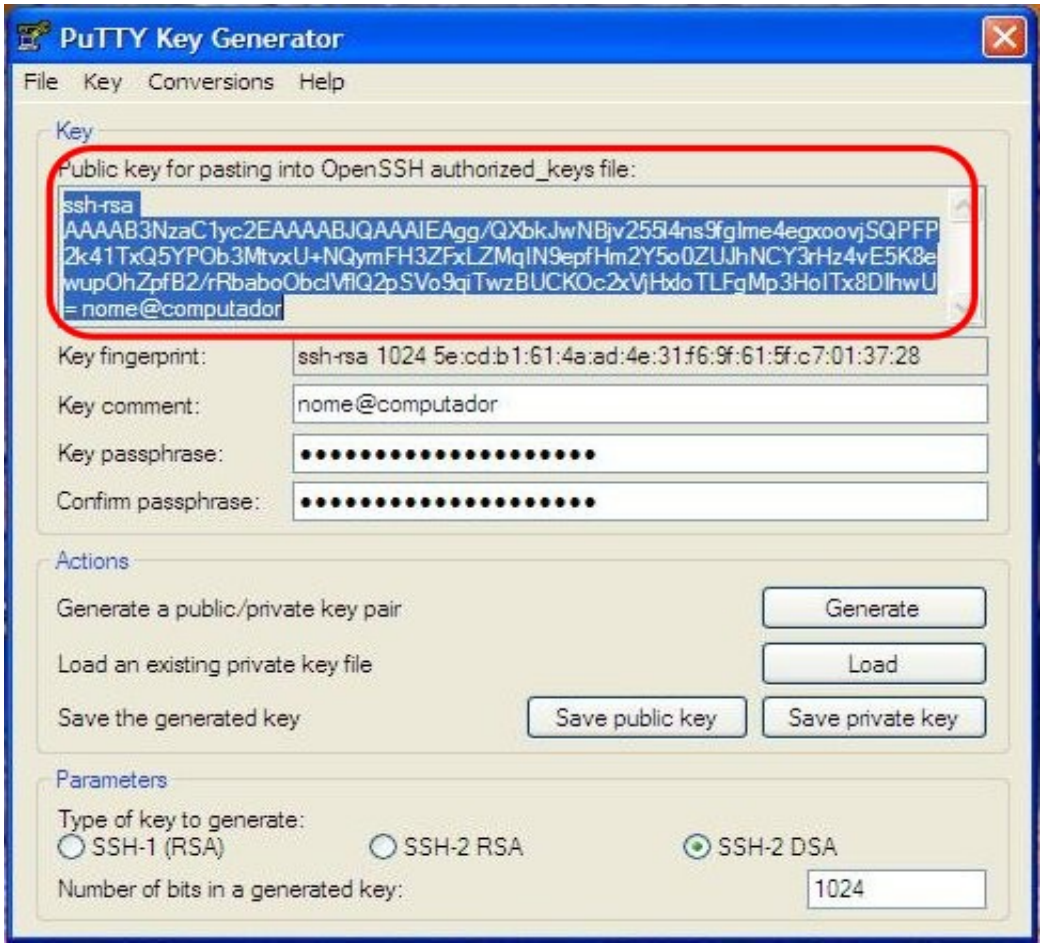
Agora escolha Save public key, para salvar sua chave pública. Escolha o local mais apropriado para guardá-la e a salve com o nome id_dsa.pub.

Faça o mesmo procedimento para Save private key, trocando o nome para id_dsa apenas. O PuTTYgen automaticamente a salvará com a extensão .ppk (PuTTY private key).



OBS.: Para a chave privada você deve se certificar de guardá-la num local seguro, onde apenas você tenha acesso. Ela é a chave principal das operações de criptografias; se outra pessoa puder acessá-la, essa outra pessoa pode atuar como um cracker, tendo acesso total a seus arquivos em outros computadores.

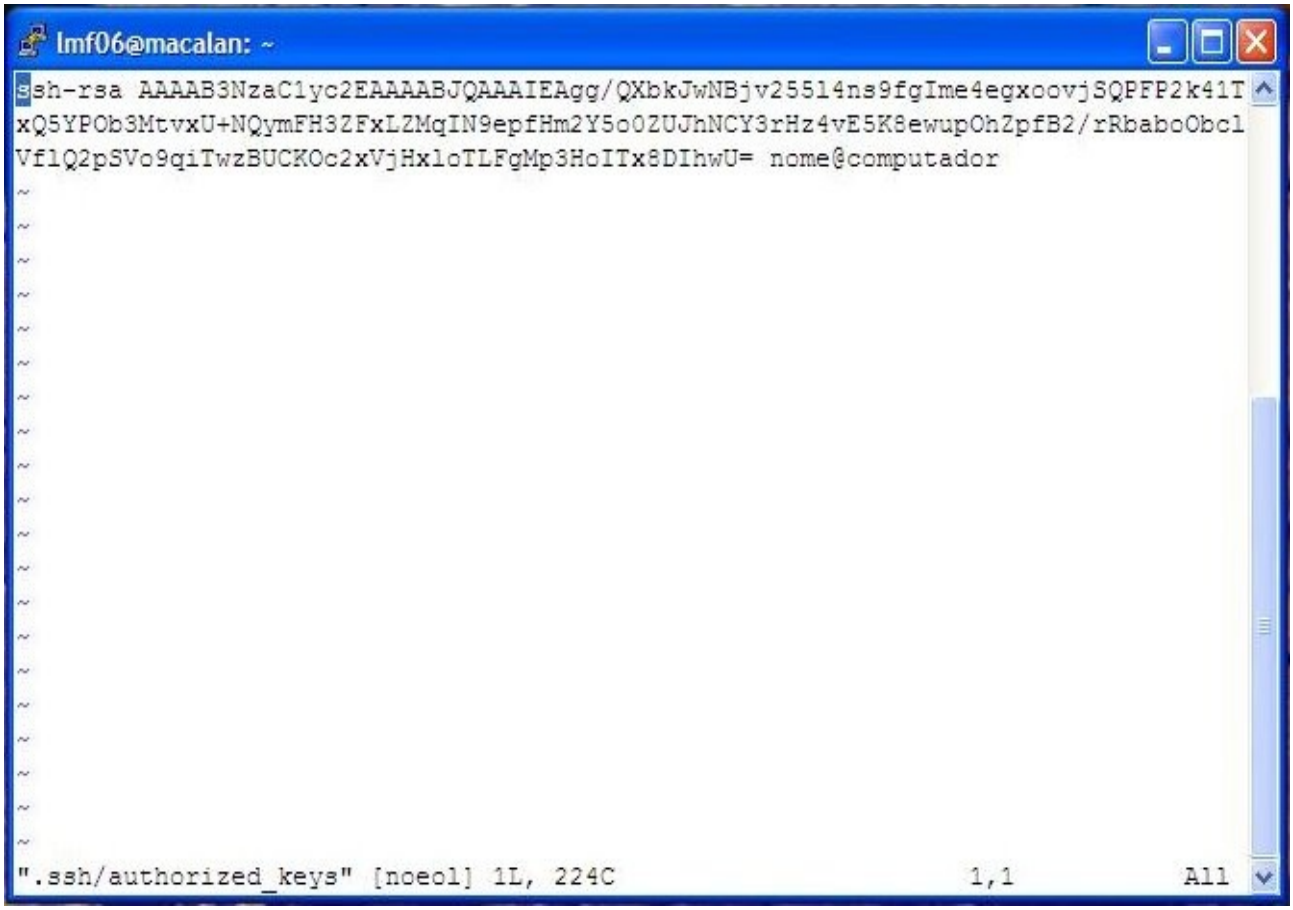

Save private key as:
Salvar em:
chaves
Documentos recentes
Desktop
Meus documentos
Meu computador
Meus locais de rede
Nome do arquivo:
id_dsa
Salvar como tipo:
PuTTY Private Key Files (*.ppk)
Salvar
Cancelar


PuTTY Key Generator
File Key Conversions Help
Key
Public key for pasting into OpenSSH authorized_keys file:
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAIEAgg/QXbkJwNBjv255l4ns9fglme4egxoovjSQPFP
2k41TxQ5YPOb3MtvxU+NQymFH3ZFxLZMqIN9epfHm2Y5o0ZUJhNCY3rHz4vE5K8e
wupOhZpfB2/rRbaboObclVfIQ2pSVo9qiTwzBUCKOc2xVjHxdoTLFgMp3HolTx8DlhwU
= nome@computador
Key fingerprint:
ssh-rsa 1024 5e:cd:b1:61:4a:ad:4e:31:f6:9f:61:5f:c7:01:37:28
Key comment:
nome@computador
Key passphrase:
Confirm passphrase:
Actions
Generate a public/private key pair
Generate
Load an existing private key file
Load
Save the generated key
Save public key
Save private key
Parameters
Type of key to generate:
SSH-1 (RSA)
SSH-2 RSA
SSH-2 DSA
Number of bits in a generated key:
1024

Você já possui seu par de chaves criado. Agora é necessário copiar sua chave pública para a máquina na qual você deseja utilizar. Para isso, copie todo o conteúdo do campo Public key for pasting into OpenSSH authorized_keys file, cole num arquivo. Esse arquivo será transferido para a máquina de destino. Utilize o scp já explicado anteriormente para isso.

Conecte-se na máquina que você deseja ter a autenticação das chaves (por SSH ou por VNC) e entre no diretório .ssh. Nesse diretório deve possuir um arquivo chamado authorized_keys, arquivo que conterá a sua chave pública. Coloque a chave que acabou de transferir com o scp e abra um editor de textos para manipular o authorized_keys. Abra também o arquivo que contenha a chave pública gerada pelo PuTTYgen.

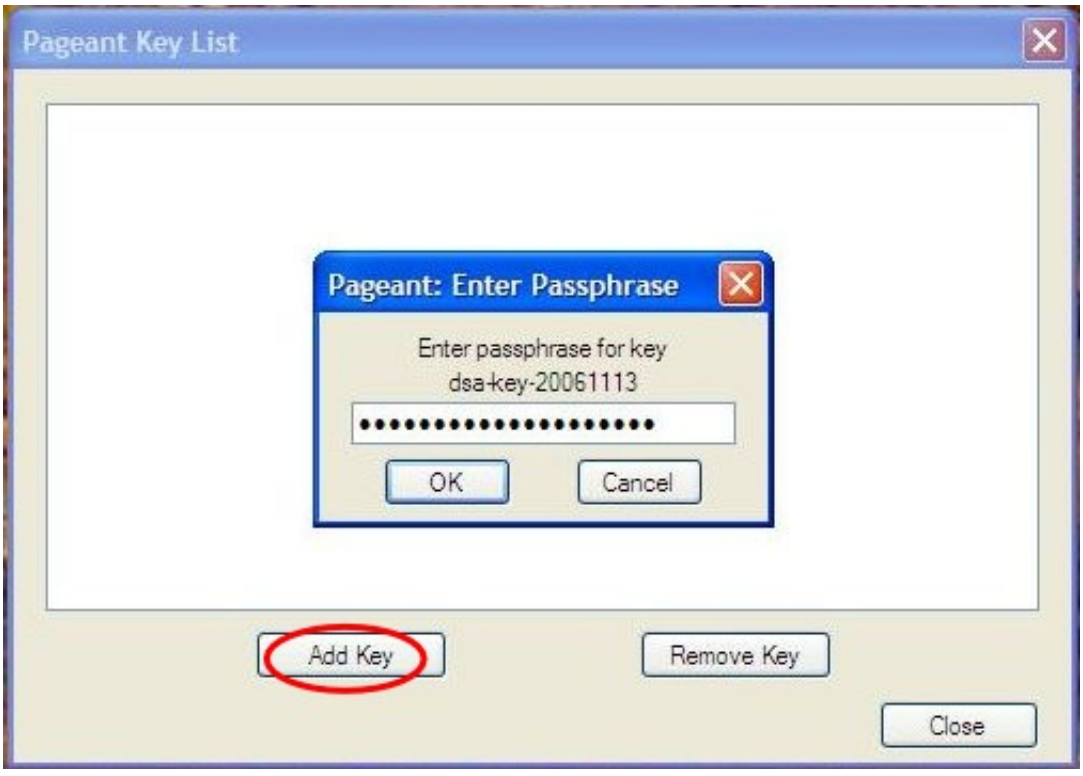
Adicione ao final do arquivo authorized_keys a sua chave pública. Lembrando que a chave pública está descrita em uma única linha, portanto deve se manter assim no arquivo authorized_keys. Salve suas alterações e retorne ao Windows.



Por último, só resta iniciar o programa Pageant. Ele é quem fará a autenticação das suas chaves geradas e lhe permitirá o acesso à máquina desejada. Assim que você o iniciar, ele será minimizado em sua barra de tarefas,

ao lado do relógio do Windows. Clique com o botão direito sobre ele e escolha View Keys.

Escolha Add Key e indique o caminho até a sua chave privada. Carregue-a e lhe será pedido para que entre com a sua chave-senha. Indique-a ao programa. Após carregada, você pode escolher Close para minimizar a janela.



Pronto! A partir de agora você pode iniciar uma sessão com o PuTTY para a máquina desejada que será usado seu par de chaves na comunicação.

OBS.: Se o procedimento estiver correto, você só precisará informar o seu usuário nas máquinas do DInf. O programa Pageant se encarrega de fazer a verificação das chaves, portanto não precisa digitar a senha.